UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,540	11/07/2003	Vincent So	79865-5 /aba	8250

7380 7590 03/10/2010

SMART & BIGGAR
P.O. BOX 2999, STATION D
900-55 METCALFE STREET
OTTAWA, ON K1P 5Y6
CANADA

EXAMINER	
AGWUMEZIE, CHARLES C	
ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
03/10/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us.mail@smart-biggar.ca

Office Action Summary	Application No.	Applicant(s)	
	10/702,540	SO, VINCENT	
	Examiner	Art Unit	
	CHARLES C. AGWUMEZIE	3685	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 December 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-23,34-36 and 38-56* is/are pending in the application.

4a) Of the above claim(s) *1, 4-15, 35-36, and 38-53* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *16-23, 34 and 54-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/7/03; 9/28/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. In view of the appeal brief filed on December 10, 2009, **PROSECUTION IS HEREBY REOPENED**. An office action is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR § 1.111 (if this Office action is non-final); or,

(2) request reinstatement of the appeal. If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR § 1.130, 1.131, or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

Status of Claims

2. Applicant's amendment filed on February 13, 2009 is acknowledged. Accordingly claims 16-23, 34, 54 and 55-56 remain pending.

Examiner's Initiated Interview

3. Examiner would like to thank Applicant's representative Jeff Slater for the attempted clarification of the claims with respect to 35 U.S.C. 112 first paragraph issues on March 4, 2010. In an attempt to justify that the specification as originally filed supports the claimed limitations of "only after" as contained in claims 16, 34 and 54, Examiner was directed to fig. 3, step 37-44 of the diagrams and pages 19-20 of the

specification. Examiner have thoroughly examined fig. 3, step 37-44 of the diagrams and pages 19-21 including any other pertinent sections of the specification and found no support for the claimed limitations "only after" as contained in claims 16, 34 and 54. Accordingly a new rejection is hereby issued with respect to the new matter.

Response to Arguments

4. Applicant's arguments with respect to claims 16-23, 34, and 54-56 have been considered but are moot in view of the new ground(s) of rejection.

5. In addition, Applicant's arguments filed February 13, 2009 have been fully considered but they are not persuasive with respect to claim 16-23, 34, 54-56.

6. With respect to **claims 16 and 34**, Applicant argues that the currently amended independent claims 16 and 34 are both novel and inventive over the cited art. Specifically that Feig does not teach or suggest that "the decryption key for a second encrypted section of video data content is received before playback of the first encrypted section of video data content is complete, and that the decryption key for the first encrypted section is not deleted until after at least the decryption key for the second encrypted section is received...

In response to applicant's arguments, and as a preliminary matter, the claimed limitation is not supported by the specification as originally filed. The specification as originally filed contains no support for **"only after"** claim phrases as contained in claims 16, 34 and 54. Examiner further disagrees and submits that Feig does disclose or teach the claimed limitation: "the decryption key for a second encrypted section of video data

content is received before playback of the first encrypted section of video data content is complete. For example Feig made it clear that the server 100 would transmit all of the token keys in a token key block, wherein each respective token key can be retrieved from the token key block at the client receiver 200 in a sequence ordered by the order of occurrence of playback of each corresponding one of the partitioned multimedia file 102. This order of occurrence would be enforced by the embedding of the sequence number in each respective token. This means that the client receiver is able to obtain the decryption key for the next encrypted section before playback of the first encrypted section is complete (see col. 7, line 35-col. 8, line 15, notice the time sensitive nature of the tokens). This is especially true where the content is a multimedia file which requires contiguous playback without which there would be disjointed playback of the multimedia content. Accordingly, under the broadest reasonable interpretation, Feig does disclose "the decryption key for a second encrypted section of video data content is received before playback of the first encrypted section of video data content is complete", otherwise there would be a lack of contiguous playback of the multimedia file.

7. Applicant further argues that Giroux et al does not teach or suggest that "the decryption key for the first encrypted section is not deleted until after at least the decryption key for the second encrypted section is received..."

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir.

1986). Applicant is reminded that Feig already has possession of the next or second set of decryption keys for the next encrypted segment before the completion of the playback of the current encrypted content. All Guiroux have to do is to provide for the deletion of the of the respective decryption keys for each segment and the process is repeated for the next segment. Thus the combination of Feig and Giroux does disclose the claimed limitation.

8. Applicant further argues that Giroux is not in any way directed to providing seamless playback of sequential contiguous sections of encrypted video data content, rather Giroux is directed to controlling access to discrete sections of content in a non-time sensitive manner.

In response Examiner respectfully disagrees with Applicant's characterization and submits that Giroux made it clear that the invention may be used in conjunction with any type of video, audio, pictorial or electronic data (see col. 2, lines 5-15). Even if Giroux is found to be controlling access to discrete sections of content in a non-time sensitive manner as Applicant appears to argue, Feig does disclose and is directed to seamless playback of sequential contiguous sections of encrypted video data content that are time sensitive (see col. 7, line 35-col. 8, line 15).

9. Applicant further argues that Giroux does not allow the viewing user to receive the decryption key for the different section until after the viewing user has finished viewing the current section.

In response, Examiner submits that even if this argument is true, Feig already has possession of the next encrypted section or segment key before the playback is

complete, thus allowing the viewing user to receive the decryption key for the different section before the viewing user has finished viewing the current section (see col. 7, line 35-col. 8, line15). This must be true in order for the client of Feig to have seamless playback of the encrypted contents. All Giroux have to do and which it does is to provide the deletion of the decryption key at the end of each segment or block.

10. Applicant further argues that Giroux's customer processing platform does not have at most a subset of the decryption keys corresponding to the plurality of encrypted sections of video data content.

In response to applicant's argument that Giroux's customer processing platform does not have at most a subset of the decryption keys corresponding to the plurality of encrypted sections of video data content, Applicant is reminded that a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. Accordingly the limitation "such that contiguous playback of the encrypted sections of video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of video data content" is an intended use recitation that simply states result. Furthermore and as argued above, Feig already has possession of the subsets of the next section keys such that contiguous playback of the encrypted sections of video data content is provided (see col. 7, line 35-col. 8, line15).

11. Applicant further argues that there is no motivation to combine the teachings of Feig with the teachings of Giroux in so far as Giroux is directed to controlling access to particular portions of non-time sensitive documents and disparate non-contiguous audi/video clips.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, both Feig and Giroux are directed to the playback of encrypted portions or sections of video data contents. Furthermore, the Examiner notes that KSR forecloses the argument that a specific teaching, suggestion, or motivation is required to support a finding of obviousness. See *KSR*, 127 S. Ct. at 1741, 82 USPQ2d at 1396.

12. With respect to **claims 17-19, 21-23 and 54**, Applicant argues that these claims are allowable by virtue of their dependency from independent claim 16.

In response, Examiner respectfully disagrees and submits that claims 17-19, 21-23 and 54 are neither patentable by virtue of their dependency from claim 16 nor for their own individual recited features.

13. With respect to **claim 20**, Applicant's argument is moot in view of new grounds of rejection.

Claim Rejections - 35 USC § 112

14. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

15. **Claims 16-23, 34, and 54-56**, are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The specification as originally filed contains no support for "destroying the respective decryption key **only after** at least a respective decryption key in respect of a next encrypted section has been received (**claim 16**); causing a key for a preceding portion of the encrypted video data to be deleted from the customer data content processing device **only after** at least the key to decrypt the subsequent portion of the encrypted data has been received by the customer data content processing device (**claim 34**); wherein destroying the respective decryption key only after at least the respective decryption key in respect of the next encrypted section has been received comprises destroying the decryption key **only after** completing playback of the encrypted section and beginning playback of the next encrypted section (**claim 54**). There are new claims without support in the specification. This is the first instance of

this invention that is unrelated and unsupported by the original filing. Cancellation of the new matter is required.

Applicant's amendments/arguments filed February 13, 2009 have been considered but are deemed without merit since the applicant argues an invention lacking support in the specification and based entirely on new matter.

Claim Rejections - 35 USC § 112

16. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

17. **Claims 16 and 34**, are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically it is would be unclear to one of ordinary skill in the art to understand which of the preceding blocks or sections of the plurality of the encrypted blocks or sections that will be completed before the next key is received. For example if you have encrypted sections 1, 2, 3, 4, ….n, all of the sections precedes n, just like encrypted section 4 precedes encrypted sections 1, 2 and 3. So which of this section need be completed before the next decryption key is received.

Dependent claims 17-23, 54-56 are also rejected for being dependent from their respectively independent claims 16 and 34.

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. **Claims 16-18**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al U.S. Patent No. 7,251,833 in view of Giroux et al U.S. Patent Application Publication No. 2002/0078361 A1.

20. As per **claims 16 and 21**, Feig et al discloses a method of receiving and controlling playback of data content at a customer processing platform, comprising:

receiving over a communications medium a plurality of encrypted sections of data content, each of which has been encrypted using a respective encryption key (fig. 3; steps 302-314; col. 1, line 55-col. 2, line 10, which discloses "plurality of sequential data blocks using corresponding token key");

and for each encrypted section:

receiving a respective decryption key in respect of the encrypted section before playback of a preceding encrypted section of the plurality of encrypted sections is complete (col. 2, lines 40-65, which discloses that "it is preferred that the token keys are transmitted to the client receiver by sequentially streaming each of the token keys, one at a time, enabling a one –to-one decryption and playback of the encrypted sequential data blocks"; col. 3, lines 1-5, which discloses that preferred method further includes

sequentially decrypting each of the respective plurality of encrypted sequential data blocks using corresponding one of the plurality of cryptographic token keys…and for playing back each recovered sequential data"; col. 7, line 35-col. 8, line15);

decrypting and playing back the encrypted section using the decryption key (col. 2, lines 40-65, which discloses that "it is preferred that the token keys are transmitted to the client receiver by sequentially streaming each of the token keys, one at a time, enabling a one –to-one decryption and playback of the encrypted sequential data blocks"; col. 3, lines 1-5, which discloses that preferred method further includes sequentially decrypting each of the respective plurality of encrypted sequential data blocks using corresponding one of the plurality of cryptographic token keys…and for playing back each recovered sequential data");

destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received, such that contiguous playback of the encrypted sections of video data is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of data content.

21. What Feig et al does not explicitly teach is

destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received, such that contiguous playback of the encrypted sections of video data is provided and at any time the customer processing platform has simultaneous possession of at most a subset of

the decryption keys corresponding to the plurality of encrypted sections of video data content.

22. Giroux et al discloses a method comprising:

destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received, such that contiguous playback of the encrypted sections of video data is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of video data content (0051, which discloses that "after decrypting the section, ... immediately discards/destroys the key...when the user moves to a different section the process is repeated...." See claim 18).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Feig et al and incorporate the method of destroying the respective decryption key only after at least a respective decryption key in respect of a next encrypted section has been received, such that contiguous playback of the encrypted sections of video data is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the plurality of encrypted sections of video data content in view of the teachings of Giroux et al in order to ensure security as well as eamless playback of the encrypted content and in addition since the claimed invention is merely a combination of old elements, and in the combination each element merely would have

performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

23. As per **claim 17**, Feig et al failed to explicitly disclose the method, further comprising, for each encrypted section:

destroying decrypted video data content at the customer processing platform after completing playback of the encrypted section.

Giroux et al discloses a method comprising destroying decrypted video data content at the customer processing platform after completing playback of the encrypted section (0051, which discloses that "after decrypting the section, ... immediately discards/destroys the key...").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Feig et al and incorporate the method of destroying decrypted video data content at the customer processing platform after completing playback of the encrypted section in view of the teachings of Giroux et al in order to ensure security and in addition since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

24. As per **claim 18**, Feig et al discloses the method, wherein the communications medium is the public Internet (col. 1, lines 40-50).

25. As per **claim 54**, Feig et al failed to explicitly disclose the method, wherein destroying the respective decryption key only after at least the respective decryption key in respect of the next encrypted section has been received comprises destroying the decryption key only after completing playback of the encrypted section and beginning playback of the next encrypted section.

Giroux et al discloses the method, wherein destroying the respective decryption key only after at least the respective decryption key in respect of the next encrypted section has been received comprises destroying the decryption key only after completing playback of the encrypted section and beginning playback of the next encrypted section (0051, which discloses that "after decrypting the section, ... immediately discards/destroys the key..."; see claim 18).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Feig et al and incorporate the method wherein destroying the respective decryption key only after at least the respective decryption key in respect of the next encrypted section has been received comprises destroying the decryption key only after completing playback of the encrypted section and beginning playback of the next encrypted section in view of the teachings of Giroux et al in oreder to ensure security of the encrypted content and in addition since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one

of ordinary skill in the art would have recognized that the results of the combination were predictable.

26. As per **claim 55**, Feig further discloses the method, further comprising, for each encrypted section:

requesting the respective decryption key in respect of a next encrypted section responsive to one of a control signal and a data pattern in the decrypted data content of an encrypted section that precedes the next encrypted section (see col. 8, lines 1-15).

27. **Claim 19**, is rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al U.S. Patent No. 7,251,833 in view of Giroux et al U.S. Patent Application Publication No. 2002/0078361 A1 and further in view of Granger et al U.S. Patent No. 6,334,189 B1.

28. As per **claim 19**, both Feig et al and Giroux et al failed to explicitly disclose the method, wherein, for each encrypted section, the respective encryption key is the same as the respective decryption key.

Granger et al discloses the method, wherein, for each encrypted section, the respective encryption key is the same as the respective decryption key (col. 10, lines 45-55, which discloses that ..."the decryption key is the same as the encryption key...").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Feig et al and incorporate the method

wherein, for each encrypted section, the respective encryption key is the same as the respective decryption key in view of the teachings of Granger et al since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

29. **Claims 22-23**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al U.S. Patent No. 7,251,833 in view of Giroux et al U.S. Patent Application Publication No. 2002/0078361 A1 and further in view of Watanabe U.S. Patent No. 7,114,073 B2

30. As per **claim 22**, both Feig et al and Giroux et al failed to explicitly disclose the method, wherein each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform.

Watanabe discloses the method, wherein each encryption key comprises a respective customer processing platform-specific key which is determined based on an IP address of the customer processing platform (col. 5, lines 17-35, which discloses that "the encryption key generating unit 105 generates the encryption key on the basis of an IP address of a user to whom the digital content is to be transmitted").

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Feig et al and incorporate the method of destroying decrypted data content at the customer processing platform after completing playback of the encrypted section in view of the teachings of Watanabe in order to ensure that content is only used by authorized users.

31. As per **claim 23**, Feig et al further discloses the method, wherein receiving each respective decryption key comprises receiving a transmission value that is determined based on the respective decryption key and a hardware identifier associated with the customer processing platform, further comprising, for each encrypted section: recovering the respective decryption key from the transmission value (col. 2, lines 40-65).

32. **Claim 20,** is are rejected under 35 U.S.C. 103(a) as being unpatentable over Feig et al U.S. Patent No. 7,251,833 in view of Giroux et al U.S. Patent Application Publication No. 2002/0078361 A1 as applied to claim 16 above, and further in view of Novak U.S. Patent Application Publication No. 2003/0097655 A1.

33. As per **claim 20**, Feig et al failed to explicitly disclose the method, wherein receiving the plurality of encrypted sections of the data content comprises receiving the plurality of encrypted sections of the video data content from another customer processing platform via a peer-to-peer network, and wherein, for each encrypted

section, the decryption key is encrypted using a public cryptographic key corresponding to a private cryptographic key known only to the customer processing platform.

Novak discloses the method, wherein receiving the plurality of encrypted sections of the data content comprises receiving the plurality of encrypted sections of the data content from another customer processing platform via a peer-to-peer network, and wherein, for each encrypted section, the decryption key is encrypted using a public cryptographic key corresponding to a private cryptographic key known only to the customer processing platform (see fig. 8, which discloses that the first license user1 may transfer his license to second user 2; 0039; 0120; 0124; 0126).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of feig et al and incorporate the method of delivering the plurality of encrypted sections from the customer processing platform to a second customer processing platform in view of the teachings of Novak in order to encourage wider distribution of content to other participants.

34. Claims **34 and 56**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Peterka et al U.S. Patent Application Publication No. 2002/0170053 A1 in view of Feig et al U.S. patent No. 7,251,833 B2 and further in view of Giroux et al U.S. Patent No. 2002/0078361 A1.

35. As per **claim 34**, Peterka et al further discloses a method for controlling use of encrypted data content downloaded to a customer data content processing device, comprising:

receiving a request comprising customer verification information from a customer data content processing device (0072; 0123; 0145);

comparing the customer verification information with corresponding stored customer information (0145); and

where the customer verification information is consistent with the stored customer verification information:

billing a usage charge to an account of the customer (figs. 8 and 9);

transmitting to the customer data content processing device a digital key to decrypt a current portion of the encrypted video data content (fig. 5; 0145); and

for each subsequent portion of the encrypted video data content:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data.

36. What Peterka et al does not explicitly teach is

for each subsequent portion of the encrypted data:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted data content before playback of a preceding portion of the encrypted video data content is complete; and

causing a key for a preceding portion of the encrypted video data to be deleted from the customer data content processing device only after at least the key to decrypt

the subsequent portion of the encrypted data has been received by the customer data content processing device, such that contiguous playback of the portions of encrypted video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the encrypted video data content.

37. Feig et al discloses:

for each subsequent portion of the encrypted video data content:

transmitting to the customer data content processing device a different key to decrypt the subsequent portion of the encrypted video data content before playback of a preceding portion of the encrypted video data content is complete (col. 2, lines 40-65, "one to one decryption"; col. 7, line 35-col. 8, line15).

38. Giroux et al discloses a method of causing a key for a preceding portion of the encrypted video data to be deleted from the customer data content processing device only after at least the key to decrypt the subsequent portion of the encrypted data has been received by the customer data content processing device, such that contiguous playback of the portions of encrypted video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the encrypted video data content (0051, which discloses that "after decrypting the section, ... immediately discards/destroys the key..."; see claim 18).

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the

method of causing a key for a preceding portion of the encrypted video data to be deleted from the customer data content processing device only after at least the key to decrypt the subsequent portion of the encrypted data has been received by the customer data content processing device, such that contiguous playback of the portions of encrypted video data content is provided and at any time the customer processing platform has simultaneous possession of at most a subset of the decryption keys corresponding to the encrypted video data content in view of the teachings of Giroux et al in order to ensure security of the encrypted video data content and in addition since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

39. As per **claim 56**, Peterka failed to explicitly disclose the method, further comprising, for each subsequent portion of the encrypted data:

receiving a request from the customer data content processing device for the different key to decrypt the subsequent portion of the encrypted data, wherein the request was generated responsive to one of a control signal and a data pattern in the decrypted data content of a preceding portion of the encrypted data content during playback of the preceding portion of the encrypted data content.

Feig further discloses the method, further comprising, for each subsequent portion of the encrypted data:

receiving a request from the customer data content processing device for the different key to decrypt the subsequent portion of the encrypted data, wherein the request was generated responsive to one of a control signal and a data pattern in the decrypted data content of a preceding portion of the encrypted data content during playback of the preceding portion of the encrypted data content (col. 7, line 35-col. 8, line15)

Accordingly it would have been obvious to one of ordinary skill in the art at time of applicant's invention to modify the method of Peterka et al and incorporate the method comprising receiving a request from the customer data content processing device for the different key to decrypt the subsequent portion of the encrypted data, wherein the request was generated responsive to one of a control signal and a data pattern in the decrypted data content of a preceding portion of the encrypted data content during playback of the preceding portion of the encrypted data content in view of the teachings of Feig in order to ensure seamless playback of the encrypted video content and in addition since the claimed invention is merely a combination of old elements, and in the combination each element merely would have performed the same function as it did separately, and one of ordinary skill in the art would have recognized that the results of the combination were predictable.

Conclusion

40. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles C. Agwumezie whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Calvin Hewitt** can be reached on **(571) 272 – 6709**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Charlie C Agwumezie/
Primary Examiner, Art Unit 3685
March 5, 2010